Anti-Virus Guidelines

1.0 Purpose

To establish requirements which must be met by all computers connected to <Agency Name> networks to ensure effective virus detection and prevention.

2.0 Scope

This policy applies to all <Agency Name> computers that are PC-based or use PC-file directory sharing. This includes, but is not limited to, desktop computers, file/ftp/tftp/proxy servers, and any PC-based equipment.

3.0 Policy

All <Agency Name> PC-based computers must have <Agency Name>'s standard, supported anti-virus software installed and scheduled to run at regular intervals. In addition, the anti-virus software and the virus pattern files must be kept up-to-date. <Agency Name>'s information security team has recommended the following processes to ensure that anti-virus software is run at regular intervals, and to keep computers virus-free.

Recommended processes to prevent virus problems:

- Always run the corporate standard.
- Run the current version and install anti-virus software updates as they become available.
- Anti-virus software is to be enabled on all workstations and servers at start-up and employ resident scanning.
- Detect and eliminate viruses on computer workstations, laptops, servers, and simple mail transfer protocol gateways.
- On servers, update virus signatures files immediately, or as soon as possible, with each new release.

- NEVER open any files or macros attached to an email from an unknown, suspicious, or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.

- Delete spam, chain, and other junk email without forwarding.

- Never download files from unknown or suspicious sources.

- Avoid direct disk-sharing with read/write access unless there is absolutely an agency requirement to do so.

- Always scan a floppy diskette from an unknown source for viruses before using it.

- Always scan any media that is brought into the agency before introducing it to the network.

Any activities with the intention to create and/or distribute malicious programs into <Agency Name>'s networks (e.g., viruses, worms, Trojan horses logic bombs, etc.) are prohibited. Virus-infected computers must be removed from the network until they are verified as virus-free. If a virus is detected on your workstation and the anti-virus software can not eliminate the virus, please contact <Agency Representative>. **DO NOT TURN OFF** your computer, it will be quarantined and taken off of the network until it can be scanned and re-imaged with the operating system image.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.